IS 11713-3 (1986): Guide for Physical Planning of Computer Complexes, Part 3: Security Considerations [LITD 11: Fibre Optics, Fibers, Cables, and Devices]

BLANK PAGE

IS : 11713 (Part 3) - 1986
(Reaffirmed 2003)

Indian Standard

GUIDE FOR PHYSICAL PLANNING OF COMPUTER COMPLEXES

PART 3 SECURITY CONSIDERATIONS

UDC 681'324 : 721'055 : 614'8

INDIAN STANDARDS INSTITUTION
MANAK BHAVAN, 9 BAHADUR SHAH ZAFAR MARG
NEW DELHI 110002

Gr 3

February 1987

Indian Standard

GUIDE FOR PHYSICAL PLANNING OF COMPUTER COMPLEXES

PART 3 SECURITY CONSIDERATIONS

(*Continued on page* 2)

(*Continued from page* 1)

Members	*Representing*
SHRI G. RAGHUKUMAR	The Delhi Cloth & General Mills Co Ltd, New Delhi
SHRI A. N. PAWAR (*Alternate*)	
SHRI C. S. RAMACHANDRAN	Reserve Bank of India, Bombay
DR J. GOPALA RAO	Electronics Corporation of India Ltd, Hyderabad
DR V. K. RAVINDRAN	PSI Data Systems Pvt Ltd, Bangalore
SHRI V. L. DESHPANDE (*Alternate*)	
RROF R. SADANANDA	Computer Society of India, Bombay
SHRI K. L. GARG (*Alternate*)	
SHRI ASHIS SEN	Indian Statistical Institute, Calcutta
SHRI UMESH P. SHAH	ORG Systems, Vadodara
SHRI P. K. SRIDHARAN (*Alternate*)	
SHRI M. SHANKRALINGAM	Directorate General of Supplies & Disposals, New Delhi
SHRI V. R. UNNIRAMAN	Telecommunication Research Centre, New Delhi
SHRI K. M. VISWANATHAN	Hindustan Teleprinters Ltd, Madras
SHRI S. DEVARAJAN (*Alternate*)	
SHRI N. SRINIVASAN, Director (Electronics)	Director General, ISI (*Ex-officio Member*)

Secretary
SHRI A. S. RAWAT
Deputy Director (Electronics), ISI

Panel for Computer Infrastructure, LTDC 24/P1

Convener	
SHRI R. THIAGARAJAN	Department of Science and Technology, New Delhi
Members	
SHRI R. K. DUTTA	Indian Meteorological Department, New Delhi
SHRI S. P. GHOTHOSKAR	Reserve Bank of India, Bombay
DR M. IBRAMSHA	Indian Institute of Technology, New Delhi
SHRI M. M. N. KAPUR	Central Statistical Organization, New Delhi
DR VINAY MATRI	School of Planning and Architecture, New Delhi
DR S. S. PILLAI	Indian Agriculture Statistical Research Institute, New Delhi
BRIG V. M. SUNDARAM	International Computers Indian Manufacturers Ltd, New Delhi

Indian Standard

GUIDE FOR PHYSICAL PLANNING OF COMPUTER COMPLEXES

PART 3 SECURITY CONSIDERATIONS

0. FOREWORD

0.1 This Indian Standard (Part 3) was adopted by the Indian Standards Institution on 23 January 1986, after the draft finalized by the Computers, Business Machines, and Calculators Sectional Committee had been approved by the Electronics and Telecommunication Division Council.

0.2 The computer system — equipment, software and information stored and under process-require to be protected against intentional or accidental damage, loss, mutilation, etc. The processed information provided by the computer systems are generally accepted without any doubt and often a deliberate or accidental manipulation may go undetected. Moreover, the sensitive electronic equipment and magnetically stored information can be accessed/damage from remote locations by tapping of communication channels.

0.3 It is obvious, therefore, that the security measures taken in a computer environment would require more attention than any other physical facilities. While security of physical facilities could be ensured through protective mechanisms devised over the years, such time tested procedures do not exist in respect of computer environments. Many organizations are yet to realise that computer systems are important corporate property and should be protected from exploitation.

0.4 In a computer environment, any activity (whether accidental or intentional), which endangers the security of accurate, speedy, and timely information is detrimental to the functioning of the management. Thus all actions taken to prevent mutilation, corruption, delay, loss, fraud and the like could be considered under security of a computer complex.

0.5 All security measures aim at achieving integrity, secracy and security. Such measures adopt a philosophy of, firstly, minimising probability of occurrence, secondly, minimising loss and damage if they occur and lastly, evolving recovery plans and contigency measures to recover loss or mutilated data.

1. SCOPE

1.1 This standard (Part 3) provides guidance for identification of areas that pose a threat to security of computer complex and guidelines to follow at planning stage for improved security.

1.2 It does not cover areas related to data security through system design, operations and similar functions.

2. TERMINOLOGY

2.1 For the purpose of this standard, the terms and definitions as given in IS : 1885 (Part 52)* of series shall apply.

3. ELEMENTS

3.0 The various security considerations in a computer complex may be discussed in three stages:

a) Planning stage,

b) Installation stage, and

c) Operation stage.

3.1 Planning Stage — During the physical planning for the establishment of computer complex, the major factors that would need to be considered are:

a) Vulnerability, and

b) Threat and risk analysis.

3.1.1 *Vulnerability* — During the planning stage, site of the computer complex assumes an important dimension mainly because, once the complex is sited and established, it would not be possible to relocate that complex easily just because some parts of the complex become vulnerable to unauthorised entry. Therefore, the planner of the computer complex would have to anticipate not only the existing flow of traffic near and around the computer complex (both pedestrian and vehicular) but also anticipate the growth of traffic over the immediate future (5 to 10 years) during which period the computer complex in its ultimate form would be established.

The computer complex could become vulnerable not only to man-made hazards such as war, riots, gherao, threat, fire, etc, but also to natural hazards such as floods, earthquake, fire, etc.

*Electrotechnical Vocabulary: Part 52 Data processing.

Some of the steps that could be taken to guard against such hazards would be to:

a) avoid locating the computer complex in very busy areas where control of movement of persons is difficult.

b) locate the computer complex away from rivers, drains, etc, which could cause damage due to floods.

c) Avoid locating the computer complex in areas which are fire prons areas such as saw-mills, fuel godowns, gas factory and so on.

d) Any other additional measures which would prevent unauthorised entry into computer complex.

3.1.2 *Threat and Risk Analysis* — Every effort must be made to assess, right at the planning stage itself, the extent of threat to the computer complex that is likely to occur. It is also important that the planner of a computer complex anticipate the risk involved in the siting, layout, actual building, operation, etc, of the computer complex. Threat to a computer complex could be posed not only by external sources but also internal ones, such as disgruntled staff who could sabotage the efforts of the organization. Accordingly, the concerned organization runs the risk of losing its computer—associated facilities due to acts of commission and omission by its own staff also.

Even though it may be a difficult task, an attempt must be made to study the extent of threat to security in every segment of the complex in order that one may arrive at various levels of danger. Such a study will also highlight the risks involved in the siting, layout, etc, of the computer complex. Thus, a systematic threat and risk analysis would facilitate the formulation of preventive steps and articulation of contingency and recovery plans.

Any attempt at conduct of threat and risk analysis for a computer complex must take not of the cost that is likely to be involved in conducting such an analysis.

Threat and risk analysis is concerned with the identification, measurement and control of uncertain events with the aim of taking decisions with regard to protection against damage, loss, etc. Such analysis must also result in formulation of contingency measures and recovery plans.

Threat and risk analysis study must include the following facts:

a) Value of the installation,

b) Likely value in terms of money and time to the recipient(s) of date,

c) Existing safeguards, and

d) Impact on the organization due to factors other than time and money.

A check list of possible threats to security of a computer complex at the time of planning is given at Appendix A.

It would be appropriate to record the various facets of threat and risk analysis and other associated measures in the form of security standing orders. Some of the sections in such security standing orders could be as given at Appendix B.

3.2 Installation Stage — Having planned the siting of a computer complex as well as other associated matters, it would be necessary to incorporate various security measures even at the time of installation of computer and associated equipment. Two major factors that are likely to have an important bearing on security of the computer complex during the installation stage are accessibility during installation and layout adopted.

3.2.1 *Accessibility* — If appropriate measures are not taken to prevent unauthorised personnel from entering the computer during the installation phase, it is likely that such personnel could —

a) Install monitoring devices such that when the computer programmes become operational, their activity could be detected through monitors; and

b) Observe the security measures being taken in the computer complex at the installation phase and use such knowledge when the system becomes operational. To avoid attracting unauthorised persons from seeking entry into the computer complex at the time of installation, it is necessary to adopt the principle of 'need to know'.

3.2.2 *Layout* — While the layout of physical devices in a computer room above ground could be observed at any point of time during the operational stage of the computer complex, layout of cables under false flooring is not normally visible to the naked eye. Therefore, it would be a good policy not to divulge the cable routing pattern during the installation phase to persons who need not know about the same.

3.2.3 In addition to the steps taken with regard to accessibility and lay-out, it would be appropriate to effectively implement orders with regard to the following:

a) Approach to the computer centre, and

b) Policy on entry. Further, installation of alarms, safety devices, fire fighting equipment, etc, also assume a special significance during this stage itself.

3.3 Operational Stage — Many of the threats to security of computer complex occur actually during the physical running of a computer

system. It behaves on the computer centre management to avoid becoming complacent in the hope that the centre has been well planned and laid out to prevent loss of security.

3.3.1 During the operational stage, not only would preventive steps pose a problem but recovery and contingency measures would also become very important. Therefore, it would be appropriate to draw up security standing orders for the computer complex as given in Appendix B.

These orders must clearly spell out the hierarchy of controls within the organization primarily from the point of view of security.

3.3.2 Once having installed the computer system and started working with the same, it is absolutely essential that periodic inspection of the various facilities is resorted to with a view to ensuring that the various components function according to their designated duties. Such periodic inspection must also incorporate an element of realism by introducing (with full prior knowledge of concerned management personnel), occurrence of loss, mutilation, etc. Such inspections would reveal any possible lapses in the security arrangements within the organization.

3.3.3 Monitoring, evaluation and review of the various security measures undertaken by the organization during the actual operation of the system become very crucial. Monitoring machanisms must be installed without undue publicity. It is quite likely that implementation of the security measures might necessitate a complete over-haul of certain procedures and organizational set up. Management of the organization must be adviced by the computer centre personnel about the need for such over-haul if found necessary.

4. SECURITY TRAINING

4.1 While orders may be written and communicated to various personnel of the organization, actual implementation would be facilitated by imparting appropriate training to the concerned personnel. Thus, security training assumes an important role during the operational stage. Such training must be made as realistic as possible and the employees being trained must be made to realize the importance of various measures instituted by the management from a security angle. It must be emphasized that a committed employee of an organization is bound to ensure the success of the organization and prevent even his own colleagues from causing loss of security of information (which is becoming the most important property of management in the modern context).

APPENDIX A

(*Clause* 3.1.2)

CHECK LIST OF THREATS TO SECURITY THAT HAVE TO BE CONSIDERED IN PLANNING A COMPUTER COMPLEX

Sl No.	*Category*	*Threat*	*Applicable to*				
			PC	LAN	MINI	MIDI	LARG
(1)	(2)	(3)	(4)	(5)	(6)	(7)	(8)
1.	Hazards	Fire	Y	Y	Y	Y	Y
		Storm/Flood	—	—	—	Y	Y
		War	—	—	—	Y	Y
		Rodents/Pests	—	Y	Y	Y	Y
		Moisture/Seepage	—	Y	Y	Y	Y
		Dust	—	—	Y	Y	Y
		Temperature	—	—	—	Y	Y
		Other Catastrophes	—	—	Y	Y	Y
2.	Hardware	Proper selection	—	Y	—	Y	Y
		Back-up system	—	—	Y	Y	Y
		Maintenance	—	—	—	Y	Y
3.	Software	Packages	Y	Y	Y	Y	Y
		Amendment	Y	Y	Y	Y	Y
		Application packages	Y	Y	Y	Y	Y
4.	Ancillaries	Media selection	Y	Y	Y	Y	Y
		Power supply	—	Y	Y	Y	Y
		Air conditioning	—	—	Y	Y	Y
5.	Communication	Modems	—	Y	Y	Y	Y
		Frames, line	—	Y	Y	Y	Y
6.	Layout, access Vulnerability		—	—	—	Y	Y
7.	Deliberate action	Looting	—	—	—	Y	Y
		Sabotage (violent like bombs, tapping, etc, or non-violent like erasure)	—	Y	Y	Y	Y

The following are not necessarily to be considered when planning the complex but will have long term effects if layout is wrong:

8.	System	Media damage	—	Y	Y	Y	Y
		Keying in error	—	Y	Y	Y	Y
		Wrong operator action	—	—	—	Y	Y
		Data transmission	—	—	—	Y	Y
		Improper testrun	—	—	—	Y	Y
		Playful damage	—	—	Y	Y	Y
		Invasion of privacy	—	—	Y	Y	Y

NOTE — PC = Personnel computer
LAN = Local area network
MINI = Mini computer
MIDI = Midi computer
LARG = Large computer

APPENDIX B

(*Clauses* 3.1.2 *and* 3.3.1)

SUGGESTED SECTIONS IN SECURITY STANDING ORDERS IN A COMPUTER COMPLEX

B-1. INTRODUCTION

B-1.1 Reference to threat and risk analysis and other studies; layout; scope, etc.

B-2. PHYSICAL SECURITY

B-2.1 Site policy; layout principles; time frames environment specifications; services specifications; standby details; guard and picquets duties, etc, passes and controls; where possible action in case of compromise, failures, etc, must be laid down.

B-3. FIRE ORDERS

B-3.1 Action on occurrence, organization, mutual assistance plans, etc; would include alarms, their siting, what to remove and safety of property and life, etc.

B-4. DATA SECURITY

B-4.1 Input criteria (unique identification, for example, check digit, serial numbering, target dates); policy on transmission; data preparation policy (error percentages, batching, hash total, etc) coding policy and schemes; training for input and coding; validation norms (manual and programmed); access restrictions; closed shop; error correction procedures; retention and back up policy; historical data; etc.

B-5. SYSTEM SECURITY

B-5.1 Selection and replacement policy; conversion policies; hardware maintenance; software maintainance; system and program identification; program modification procedures; system initiation and amendment; data base policy; pass-word and security policy.

B-6. COMMUNICATION

B-6.1 Protocol policy; procedure for acquiring and releasing data circuits; monitoring policy; measures to inhibit tapping/eaves dropping; encryption policy, if applicable; speeds of operation; detection and rectification of breakdowns, etc.

B-7. PRIVACY

B-7.1 Government regulations and organization's policy; authentication procedure; documentation, etc.

B-8. ORGANIZATION

B-8.1 Hierarchy of control; reporting mode; officiating arrangements in case of absence; job specifications, etc.